PUPA 2002-542546

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G07F 19/00, 17/16, G06F 1/00 — A1

(11) Numéro de publication internationale: **WO 00/63859**

(43) Date de publication internationale: 26 octobre 2000 (26.10.00)

(21) Numéro de la demande internationale: PCT/FR00/01023

(22) Date de dépôt international: 19 avril 2000 (19.04.00)

(30) Données relatives à la priorité:
99/04963 20 avril 1999 (20.04.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean-Claude [FR/FR]; 4, rue des Loisirs, F-14610 Epron (FR). MICHON, Philippe [FR/FR]; 96, avenue H. Cheron, F-14000 Caen (FR). PETIT, Stéphane [FR/FR]; App. 146, Bât Les Iris, Résidence du Nouveau Bassin, 32, rue de Ver, F-14470 Courseulles/Mer (FR).

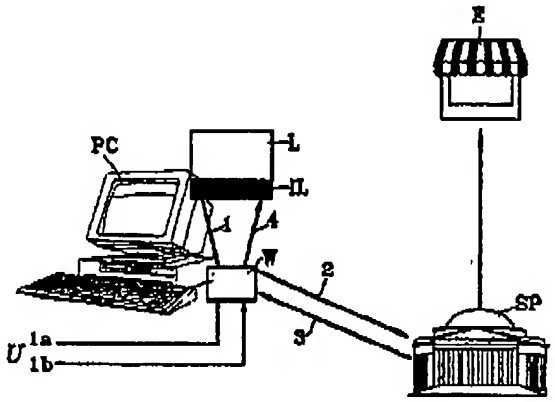
(74) Mandataire: POULIN, Gérard; Société de Protection des Inventions, 3, rue du Docteur Lancereaux, F-75008 Paris (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, RU, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: PAYMENT SYSTEM FOR SOFTWARE USE

(54) Titre: SYSTEME DE PAIMENT POUR L'UTILISATION DE LOGICIELS



(57) Abstract

The invention concerns a payment system for use of software, comprising an software interface (IL), a payment module (W), a payment server (SP) connected to the software editor (E). The offer for use consists in a message (2), a payment request (2), a payment (3), (4). The invention is useful for controlling the use of software.

(57) Abrégé

Système de paiement pour l'utilisation d'un logiciel. Le système comprend une interface logicielle (IL), un module de paiement (W), un serveur de paiement (SP) en liaison avec l'éditeur du logiciel (E). L'offre d'utilisation fait l'objet d'un message (2), d'une demande de paiement (2), d'un acquittement (3, 4). Application au contrôle de l'utilisation des logiciels.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G07F 19/00, 17/16, G06F 1/00	A1	(11) Numéro de publication internationale: **WO 00/63859** (43) Date de publication internationale: 26 octobre 2000 (26.10.00)

(21) Numéro de la demande internationale: PCT/FR00/01023

(22) Date de dépôt international: 19 avril 2000 (19.04.00)

(30) Données relatives à la priorité:
99/04963 20 avril 1999 (20.04.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean–Claude [FR/FR]; 4, rue des Loisirs, F–14610 Epron (FR). MICHON, Philippe [FR/FR]; 96, avenue H. Cheron, F–14000 Caen (FR). PETIT, Stéphane [FR/FR]; App. 146, Bât Les Iris, Résidence du Nouveau Bassin, 32, rue de Ver, F–14470 Courseules/Mer (FR).

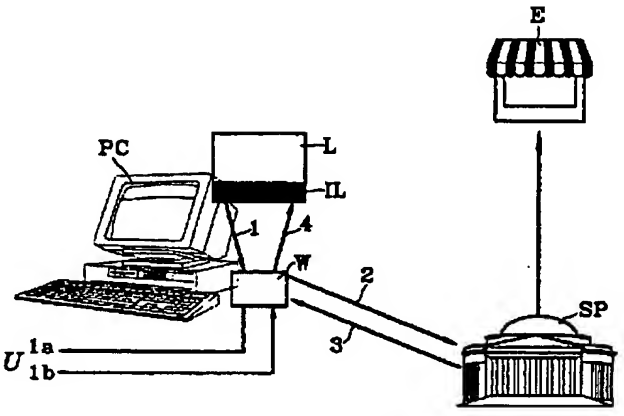
(74) Mandataire: POULIN, Gérard; Société de Protection des Inventions, 3, rue du Docteur Lancereaux, F–75008 Paris (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, RU, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: PAYMENT SYSTEM FOR SOFTWARE USE

(54) Titre: SYSTEME DE PAIMENT POUR L'UTILISATION DE LOGICIELS



(57) Abstract

The invention concerns a payment system for use of software, comprising an software interface (IL), a payment module (W), a payment server (SP) connected to the software editor (E). The offer for use consists in a message (2), a payment request (2), a payment (3), (4). The invention is useful for controlling the use of software.

(57) Abrégé

Système de paiement pour l'utilisation d'un logiciel. Le système comprend une interface logicielle (IL), un module de paiement (W), un serveur de paiement (SP) en liaison avec l'éditeur du logiciel (E). L'offre d'utilisation fait l'objet d'un message (2), d'une demande de paiement (2), d'un acquittement (3, 4). Application au contrôle de l'utilisation des logiciels.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－542546
（P2002－542546A）
(43)公表日　平成14年12月10日(2002.12.10)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０５８
17/60	３０２		３３２	５Ｂ０７６
	３３２	Ｇ０６Ｋ　17/00	Ｒ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｆ　9/06	６６０Ｃ	
			６６０Ｅ	

審査請求　未請求　予備審査請求　有　（全 26 頁）

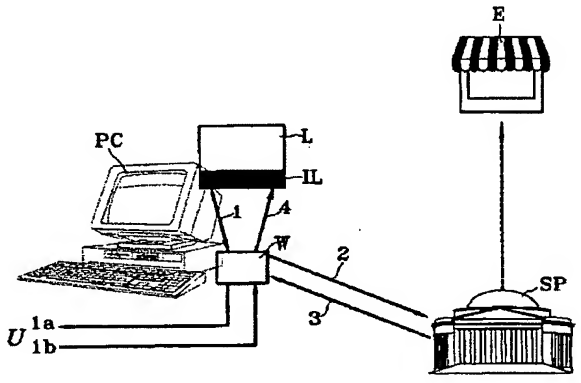
(21)出願番号　特願2000－612904(P2000－612904)
(86)(22)出願日　平成12年４月19日(2000.4.19)
(85)翻訳文提出日　平成13年10月19日(2001.10.19)
(86)国際出願番号　ＰＣＴ／ＦＲ００／０１０２３
(87)国際公開番号　ＷＯ００／６３８５９
(87)国際公開日　平成12年10月26日(2000.10.26)
(31)優先権主張番号　９９／０４９６３
(32)優先日　平成11年４月20日(1999.4.20)
(33)優先権主張国　フランス（ＦＲ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＣＮ，ＩＮ，ＪＰ，ＲＵ，ＵＳ

(71)出願人　フランス　テレコム
ＦＲＡＮＣＥ　ＴＥＬＥＣＯＭ
フランス国、75015　パリ、プラス・ダルレ、６
(72)発明者　ジャン－クロード・パイル
フランス・Ｆ－14610・ウプロン・リュ・デ・ロワシル・４
(72)発明者　フィリップ・ミション
フランス・Ｆ－14000・カーン・アヴニュ・アッシュ・シェロン・96
(74)代理人　弁理士　志賀　正武　（外７名）

最終頁に続く

(54)【発明の名称】　ソフトウェアプログラムの使用に対する支払システム

(57)【要約】
本発明による支払システムは、ソフトウェアインターフェース（ＩＬ）と、支払モジュール（Ｗ）と、ソフトウェア編集者（Ｅ）に対して接続されている支払サーバ（ＳＰ）と、から構成されている。ソフトウェアの使用申込は、メッセージ（１）の主題であり、これに対応して支払要求メッセージ（２）が送信され、さらに、支払決定メッセージ（３，４）が送信される。本発明は、ソフトウェアプログラムの使用の制御に応用することができる。



【特許請求の範囲】

【請求項１】　媒体上に搭載されるとともにインターフェース（ＩＬ）を有したソフトウェアプログラム（Ｌ）の使用に対する支払システムであって、

支払モジュール（Ｗ）と、メッセージ送受信可能な支払手段（ＳＰ）と、を具備してなり、

前記ソフトウェアインターフェース（ＩＬ）は、前記ソフトウェアの使用を申し込む第１メッセージ（１）を作成することができ、

該第１メッセージ（１）は、特に、ソフトウェア編集者（Ｅ）の識別子と、申込パラメータと、申し込まれたソフトウェアの少なくとも一部に対しての編集者のデジタル署名と、を有しているとともに、前記支払モジュールに対して送信され、

前記支払モジュール（Ｗ）は、前記第１メッセージ（１）を受領することができるとともに、前記第１メッセージを表示する（１ａ）ことができ、さらに、ソフトウェアの使用者（Ｕ）が了解した場合には、前記ソフトウェア使用者（Ｕ）の了解（１ｂ）を受領するとともに、特に前記使用者（Ｕ）の識別子と前記ソフトウェア編集者（Ｅ）の識別子と前記使用者による申込の了解を示す証明書とを有してなる支払要求を表す第２メッセージ（２）を作成することができ、

前記モジュール（Ｗ）は、さらに、前記第２メッセージ（２）を、前記メッセージ送受信可能な支払手段（ＳＰ）に対して送信することができ、

前記メッセージ送受信可能な支払手段（ＳＰ）は、前記第２メッセージ（２）を受領することができるとともに、前記第２メッセージ内の前記証明書をチェックすることができ、前記使用者（Ｕ）の識別子と前記ソフトウェア編集者の識別子と支払うべき価格とを少なくとも有している支払要求を記録することができ、さらに、その価格を当該ソフトウェア編集者に割り当てることができ、

前記メッセージ送受信可能な支払手段（ＳＰ）は、さらに、支払決定メッセージ（３）を作成することができ、

該支払決定メッセージ（３）は、特に、前記支払手段の識別子と、支払の証明をなすデジタル署名と、を有してなり、前記支払モジュール（Ｗ）へと送信され、

前記支払モジュール（W）は、付加的に、前記支払決定メッセージ（３）を、前記ソフトウェアインターフェース（ＩＬ）に対して送信することができ、

前記ソフトウェアインターフェース（ＩＬ）は、付加的に、前記支払手段のデジタル署名を、前記第１メッセージ（１）内の申込内容と照合することができ、これらが一致している場合に、前記ソフトウェアプログラム（Ｌ）の使用を承認するという機能を有していることを特徴とするシステム。

【請求項２】　請求項１記載のシステムにおいて、

前記編集者によるデジタル署名と前記支払証明書をなすデジタル署名との双方が、証明ツリーを有した一般キー署名であり、

権威者（Ａ）が、前記システムの様々な構成要員を有してなる証明ツリーの根源を規定し、

この場合の構成要員とは、特に、前記ソフトウェア編集者（Ｅ）と、前記支払手段（ＳＰ）と、であり、

前記第１メッセージ（１）および前記支払決定メッセージ（３）には、署名のチェックのために、１つまたは複数の証明書が添付されていることを特徴とするシステム。

【請求項３】　請求項１記載のシステムにおいて、

前記メッセージ送受信可能な支払手段（ＳＰ）は、遠隔通信ネットワークを介して前記支払モジュール（W）に対して接続された遠隔支払サーバ（ＳＰ）であり、

前記サーバ（ＳＰ）は、前記第２メッセージを受領してこの第２メッセージを処理し、前記支払決定メッセージ（３）を作成して送信し、

前記支払サーバは、すべてのソフトウェア編集者に関して、各使用者の合計消費時間を計算し、これにより、前記使用者に課金するとともに、各ソフトウェア編集者に関しての合計金額を、使用者のすべてから送信させることを特徴とするシステム。

【請求項４】　請求項１記載のシステムにおいて、

前記メッセージ送受信可能な支払手段（ＳＰ）は、前記使用者（Ｕ）の識別子を少なくとも有した静止手段（ＬＣ，Ｃ）を備え、

これら静止手段は、付加的に、前記第２メッセージ（２）を受領することができるとともに、該第２メッセージ内の前記証明書をチェックすることができ、さらに、支払要求を記録することができ、さらに、前記支払決定メッセージ（３）を作成することができ、

前記メッセージ送受信可能な支払手段は、さらに、前記ソフトウェア編集者（Ｅ）を認証することができる遠隔支払サーバ（ＳＰ）を備えていることを特徴とするシステム。

【請求項５】　請求項４記載のシステムにおいて、

前記静止手段は、ＩＣカード読取器（ＬＣ）と、前記使用者の識別子を有したＩＣカード（Ｃ）と、を備え、

前記読取器および前記カードは、前記第２メッセージ（２）を受領することができるとともに、該第２メッセージ内の前記証明書をチェックすることができ、さらに、支払要求を記録することができ、さらに、支払の証明書を有した前記支払決定メッセージ（３）を作成することができることを特徴とするシステム。

【請求項６】　請求項５記載のシステムにおいて、

前記カード（Ｃ）が、前払いタイプのものであって、残高を有し、

前記カードが、前記支払要求ごとに、前記要求価格を前記残高から引き落とすことができるようになっていることを特徴とするシステム。

【請求項７】　請求項６記載のシステムにおいて、

前記支払決定メッセージを作成する前記前払い式カード（Ｃ）が、前記要求価格が既に前記残高から引き落とされたことを示す証明書を有することができるようになっていることを特徴とするシステム。

【請求項８】　請求項６記載のシステムにおいて、

前記前払い式カード（Ｃ）が、決定された要求と対応する価格とを有するファイルを作成することができ、

前記支払決定メッセージが、前記ファイルが更新された後にだけ、前記デジタル署名を有して送信されるようになっていることを特徴とするシステム。

【請求項９】　請求項８記載のシステムにおいて、

前記前払い式カード（Ｃ）が、補給することができ、

前記カードが有している前記ファイルが、前記ソフトウェア編集者に対しての資金移動のために、補給プロセス時にはまず最初に前記支払サーバ（ＳＰ）に対して転送されるようになっていることを特徴とするシステム。

【請求項１０】　請求項６記載のシステムにおいて、

前記前払い式カード（Ｃ）が、『電子財布』タイプのものとされていることを特徴とするシステム。

【請求項１１】　請求項５記載のシステムにおいて、

前記カード（Ｃ）が、後払いタイプのものとされていることを特徴とするシステム。

【請求項１２】　請求項１１記載のシステムにおいて、

前記後払い式カード（Ｃ）が、決定された要求と対応する価格とを有するファイルを作成することができ、

前記支払決定メッセージが、前記ファイルが更新された後にだけ、前記デジタル署名を有して送信されるようになっていることを特徴とするシステム。

【請求項１３】　請求項１２記載のシステムにおいて、

前記カードのファイルが、前記ソフトウェア編集者に対しての資金移動のために、前記支払サーバ（ＳＰ）に対して転送されるようになっていることを特徴とするシステム。

【請求項１４】　ソフトウェアプログラムの使用に対する支払システムのための支払モジュール（Ｗ）であって、

－特にソフトウェア編集者（Ｅ）の識別子とソフトウェア使用のための申込パラメータと申し込まれたソフトウェアの少なくとも一部に対してのデジタル署名とを有している第１メッセージ（１）の処理手段と；

－使用者に対して前記第１メッセージを表示するための手段（１ａ）と；

－前記ソフトウェア使用者（Ｕ）の了解（１ｂ）を受領するための手段と；

－特に前記使用者（Ｕ）の識別子と前記ソフトウェア編集者（Ｅ）の識別子と前記使用者による申込の了解を示す証明書とを有してなる支払要求を表す第２メッセージ（２）を作成するための手段と；

－支払の証明をなすデジタル署名を有した支払決定メッセージ（３）を受領し

て処理するための手段と；

を具備してなることを特徴とする支払モジュール。

【請求項１５】　ソフトウェアプログラムの使用に対する支払システムのためのメッセージ送受信可能な支払手段（ＳＰ）であって、

－特に使用者（Ｕ）の識別子とソフトウェア編集者（Ｅ）の識別子と使用者がソフトウェア使用を承認したことを示す証明書とを有した支払要求メッセージを、支払モジュール（Ｗ）から受領するための手段と、

－前記証明書をチェックするための手段と；

－少なくとも使用者（Ｕ）の識別子とソフトウェア編集者（Ｅ）の識別子と支払うべき価格と該価格を前記ソフトウェア編集者（Ｅ）が認証するための手段とを有した支払要求を記録するための手段と；

－特に前記支払手段の識別子と支払の証明をなすデジタル署名とを有してなる支払決定メッセージ（３）を作成するための手段と；

－支払モジュール（Ｗ）に対して前記支払決定メッセージ（３）を送信するための手段と；

を具備してなることを特徴とするメッセージ送受信可能な支払手段。

【請求項１６】　ソフトウェアプログラムの使用に対する支払システムのためのメッセージ送受信可能な支払手段（ＳＰ）であって、

ＩＣカード読取器（ＬＣ）と、ソフトウェア使用者の識別子を有したＩＣカード（Ｃ）と、を備えてなる静止手段を具備し、

前記読取器および前記カードは、使用者がソフトウェア使用申込を承認したことを示す証明書を有したメッセージを受領することができるとともに、その証明書をチェックすることができ、さらに、支払要求を記録することができ、さらに、支払の証明書を有した支払決定メッセージ（３）を作成することができることを特徴とするメッセージ送受信可能な支払手段。

【請求項１７】　請求項１６記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記カード（Ｃ）が、前払いタイプのものであって、残高を有し、

前記カードが、前記支払要求ごとに、前記要求価格を前記残高から引き落とす

ことができるようになっていることを特徴とするメッセージ送受信可能な支払手段。

【請求項１８】　請求項１７記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記支払決定メッセージを作成する前記前払い式カード（Ｃ）が、前記要求価格が既に前記残高から引き落とされたことを示す証明書を有することができるようになっていることを特徴とするメッセージ送受信可能な支払手段。

【請求項１９】　請求項１７記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記前払い式カード（Ｃ）が、決定された要求と対応する価格とを有するファイルを作成することができ、

前記支払決定メッセージが、前記ファイルが更新された後にだけ、前記デジタル署名を有して送信されるようになっていることを特徴とするメッセージ送受信可能な支払手段。

【請求項２０】　請求項１７記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記前払い式カード（Ｃ）が、補給することができ、

前記ファイルが、補給プロセス時には転送されるようになっていることを特徴とするメッセージ送受信可能な支払手段。

【請求項２１】　請求項１７記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記前払い式カード（Ｃ）が、『電子財布』タイプのものとされていることを特徴とするメッセージ送受信可能な支払手段。

【請求項２２】　請求項１６記載のメッセージ送受信可能な支払手段（ＳＰ）において、

前記カード（Ｃ）が、後払いタイプのものとされていることを特徴とするメッセージ送受信可能な支払手段。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明の目的は、ソフトウェアプログラムの使用に対する支払システムを提供することである。この場合のソフトウェアは、任意のタイプのソフトウェアとすることができ、例えば、ＣＤ－ＲＯＭ（コンパクトディスク読取専用メモリ）やＤＶＤ－ＲＯＭ（デジタル多機能ディスク読取専用メモリ）といったような媒体上に記録されているソフトウェアとすることも、ダウンロードしたソフトウェアとすることも、できる。

【０００２】

ソフトウェアは、科学計算や、ゲームや、コンピュータ支援技術や、ワープロ、等に関するものとすることができる。

【０００３】

【従来の技術】

ＣＤ－ＲＯＭは、現在では、ソフトウェアプログラム流通の主要方法であり、近いうちに、ＤＶＤ－ＲＯＭによって取って代わられるであろう。ソフトウェア編集者にとって、ソフトウェアの不正コピーは、しだいに深刻な問題となってきている。ブランクディスク上へのコピーが禁止されたＣＤ－ＲＯＭフォーマットもあるにはあるけれども、一般消費者市場においては、使用者による書込が可能なディスクやＣＤ書込器が、利用可能である。同じ現象は、ＤＶＤ技術に関しても、近いうちに間違いなく起こるであろう。

【０００４】

性能の理由からあまり一般的ではないけれども、ソフトウェア流通の他の可能な方法は、ダウンロードである。この方法は、多数の像や３次元画像を必要とするゲームには適切ではない。ところが、例えば多数のソフトウェアプログラム（プログラムコンパイラ、エディタ、等）といったような他のソフトウェアの場合には、非常に好適である。一般に、これらソフトウェアプログラムは、無料である。その理由は、これらソフトウェアプログラムのサイズが小さい（ダウンロードを可能とするため）ことのために、これらソフトウェアプログラムが、コンピ

ュータどうしの間において非常に容易にコピーされ得るからである。

【０００５】

さらに、ソフトウェアプログラムの購入価格が高いことが、多くの場合、使用者に対しての躊躇をもたらしていることは、明白である。ＣＤ－ＲＯＭ自体のコストや書込コストは、価格のうちの非常に小さな部分でしかない。実際、現在のＣＤ－ＲＯＭやＤＶＤ－ＲＯＭの購入価格の高さは、主に、ソフトウェア編集者やゲーム販売者に対しての支払に対応している。

【０００６】

このような考察により、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ媒体上のソフトウェアやダウンロードしたソフトウェアに関して、使用ごとのあるいは期間ごとのあるいは利用可能期間ごとの支払が要望されるという結論が得られる。その場合、ソフトウェア編集者は、そのソフトウェアを使用した消費者の使用に応じて、より広範な使用者層から支払を受領することとなる。世界的に、そのようなプロセスが、ソフトウェア産業において販売を増大させるべきである。加えて、ソフトウェアを使用するごとに支払を行う必要があることから、ソフトウェア媒体をコピーする必要がなくなる。

【０００７】

【発明が解決しようとする課題】

しかしながら、現在のところ、ソフトウェアプログラムの使用に対する支払を信頼性高くかつ確実に行う手段が存在していない。本発明の目的は、このような課題を正確に解決することである。

【０００８】

【課題を解決するための手段】

ソフトウェアプログラムの使用に対する支払システムは、少なくとも３つの機能を満足しなければならない。すなわち、

－ソフトウェアの稼働中において、定期的に、または、ソフトウェアにおける特定事象の発生時ごとに（例えば、ゲームにおける『面』の更新時、ゲームや映画における次なる操作への更新時、等）、ソフトウェアの使用を制御できなければならない。そのような場合には、ソフトウェアは、使用料金を要求しなければ

ならない。

－使用者に対して課金するために、ソフトウェアが使用された回数を記録しなければならない。使用者が支払要求を承認した場合には、使用者に後で支払を行わさせるために、支払要求は、確実に記録されなければならない。セキュリティ特性により、使用者による請求の消去を防止しなければならない。据置支払内の少額の料金を集計することができなければならない。その結果、使用者は、実用的な理由と、そのような少額の料金を徴収するのにかかるコストによる理由と、の双方から、定期的に（例えば、１ヶ月ごとに）請求書全体を提示される。

－借りている料金を、ソフトウェア編集者に対して定期的に転送できなければならない。

【０００９】

これら機能は、いくつかの制約を満たしつつ、行われなければならない。

－ＣＤ－ＲＯＭが、外国産のものとすることができること。すなわち、ソフトウェア支払システムが、国境を跨ぐ特性を有していなければならず、そのため、機構が、国際的に延出可能であるとともに、標準化組織によって国際的に認識されるものでなければならない。

－ソフトウェア提供者がソフトウェア使用に対応した支払論理をプログラムする必要がないように、ソフトウェアと支払手段との間に、標準的なインターフェースが存在しなければならない。

－ソフトウェアの使用回数を記録するシステムが、世界中のどの国においても、ソフトウェア編集者に対しての国際的な支払を請求できなければならない。

－使用者に支払を集計して、ソフトウェア編集者に対して転送できなければならない。上述したように、これは、支払を単純化する目的のためである。また、銀行の手数料を低減するためでもある。特に、複数の国にわたる支払実行の場合には、この観点からは、少額の合計金額に対して、あまりに多数回の支払を実行することは、不合理である。

【００１０】

本発明は、上記すべての要求を満たすとともに、上記すべての制約を満たすものである。この目的のために、本発明によるシステムは、支払モジュールと、メ

ッセージ送受信可能な支払手段と、を具備して構成されている。さらに、使用制御対象をなすソフトウェアが、ソフトウェアインターフェースを有している。これら各手段の機能は、以下の通りである。

－ソフトウェアインターフェースは、ソフトウェアの使用を申し込む第１メッセージを作成することができる。この第１メッセージは、特に、ソフトウェア編集者の識別子と、申込パラメータと、申し込まれたソフトウェアの少なくとも一部に対しての編集者のデジタル署名と、を有しているとともに、支払モジュールに対して送信される。

－支払モジュールは、第１メッセージを受領することができるとともに、第１メッセージを表示することができ、さらに、ソフトウェアの使用者が了解した場合には、ソフトウェア使用者の了解を受領するとともに、特に使用者の識別子とソフトウェア編集者の識別子と使用者による申込の了解を示す証明書とを有してなる支払要求を表す第２メッセージを作成することができる。支払モジュールは、第２メッセージを、メッセージ送受信可能な支払手段に対して送信することができる。

－メッセージ送受信可能な支払手段は、第２メッセージを受領することができるとともに、第２メッセージ内の証明書をチェックすることができ、使用者（Ｕ）の識別子とソフトウェア編集者の識別子と支払うべき価格とを少なくとも有している支払要求を記録することができ、さらに、その価格を当該ソフトウェア編集者に割り当てることができ、さらに、支払決定メッセージを作成することができる。この支払決定メッセージは、特に、支払手段の識別子と、申込に対してのデジタル署名と、を有してなり、支払モジュールへと送信される。

－支払モジュールは、さらに、支払決定メッセージを、ソフトウェアインターフェースに対して送信することができる。

－ソフトウェアインターフェースは、さらに、支払手段のデジタル署名を、第１メッセージ内の申込内容と照合することができ、これらが一致している場合に、ソフトウェアプログラムの使用を承認することができる。

【００１１】

第１実施形態においては、メッセージ送受信可能な支払手段は、遠隔通信ネッ

トワークを介して支払モジュールに対して接続された遠隔支払サーバから構成され、この支払サーバは、第２メッセージを受領してこの第２メッセージを処理し、支払決定メッセージを作成して送信する。支払サーバは、すべての料金を集計し、これにより、ソフトウェア編集者に対して、借入金を定期的に報告する。

【００１２】

第２実施形態においては、メッセージ送受信可能な支払手段は、使用者の識別子を少なくとも有した静止手段を備えている。これら静止手段は、付加的に、第２メッセージを受領することができるとともに、第２メッセージ内の証明書をチェックすることができ、さらに、支払要求を記録することができ、さらに、支払決定メッセージを作成することができる。メッセージ送受信可能な支払手段は、さらに、ソフトウェア編集者を認証することができる遠隔支払サーバを備えている。

【００１３】

変形例においては、静止手段は、ＩＣカード読取器と、使用者の識別子を有したＩＣカードと、を備えることができる。カードは、第２メッセージを受領することができるとともに、第２メッセージ内の証明書をチェックすることができ、さらに、支払要求を記録することができ、さらに、支払の証明書を有した支払決定メッセージを作成することができる。

【００１４】

サーバは、ソフトウェアプログラムの使用に対応した、カード内に記録されているすべての要求を、遠隔通信ネットワークを介して、定期的に更新する。

【００１５】

カードは、前払いタイプのもの（例えば、電子財布の形態）とも、後払いタイプのものとも、することができる。

【００１６】

前払い式カードと後払い式カードとの双方は、決定された要求と対応する価格とを有するファイルを作成することができ、支払決定メッセージは、ファイルが更新された後にだけ、デジタル署名を有して送信されるようになっている。

【００１７】

また、本発明の目的は、ソフトウェアプログラムの使用に対する支払システムのための支払モジュールであって、

－特にソフトウェア編集者の識別子とソフトウェア使用のための申込パラメータと申し込まれたソフトウェアの少なくとも一部に対してのデジタル署名とを有している第１メッセージの処理手段と；

－使用者に対して第１メッセージを送信するための手段と；

－ソフトウェア使用者の了解を受領するための手段と；

－特に使用者の識別子とソフトウェア編集者の識別子と使用者による申込の了解を示す証明書とを有してなる支払要求を表す第２メッセージを作成するための手段と；

－支払の証明をなすデジタル署名を有した支払決定メッセージを受領して処理するための手段と；

を具備してなることを特徴とする支払モジュールを提供することである。

【００１８】

また、本発明の目的は、ソフトウェアプログラムの使用に対する支払システムのためのメッセージ送受信可能な支払手段であって、

－特に使用者の識別子とソフトウェア編集者の識別子と使用者がソフトウェア使用を承認したことを示す証明書とを有した支払要求メッセージを、支払モジュールから受領するための手段と、

－証明書をチェックするための手段と；

－少なくとも使用者の識別子とソフトウェア編集者の識別子と支払うべき価格とこの価格をソフトウェア編集者が認証するための手段とを有した支払要求を記録するための手段と；

－特に支払手段の識別子と支払の証明をなすデジタル署名とを有してなる支払決定メッセージを作成するための手段と；

－支払モジュールに対して支払決定メッセージを送信するための手段と；

を具備してなることを特徴とするメッセージ送受信可能な支払手段を提供することである。

【００１９】

【発明の実施の形態】

図１は、ＰＣに適合したパーソナルコンピュータを示しており、このパーソナルコンピュータは、使用の制御対象をなすソフトウェアプログラム（Ｌ）を搭載している。このソフトウェアプログラムは、以下『購買』と称するソフトウェアインターフェース（ＩＬ）と結合している。ソフトウェアインターフェースは、支払システム自体と接続している。図１には、さらに、以下『財布』と称する支払モジュール（Ｗ）が示されている。図１には、さらに、伝達ライン（図示せず）を介して財布モジュールに対して接続された遠隔支払サーバ（ＳＰ）が示されている。ソフトウェア編集者は、記号（Ｅ）によって示されている。

【００２０】

図１に示す実施形態においては、ソフトウェアプログラム（Ｌ）に対しての新たな支払が決定された時点で、符号（１）によって示されている申込メッセージが、購買インターフェース（ＩＬ）によって、財布モジュール（Ｗ）へと送信される。この申込メッセージは、以下のものを有することができる。すなわち、

－ソフトウェア編集者の識別子と；

－支払に対して使用者が見返りに得ることとなる内容（例えば、『３０分の延長使用』とか、『第３シーン：長さ２５分』とか）を説明している申込要項と；

－価格（金額、通貨、等）と；

－パーソナルコンピュータ（ＰＣ）の内部クロックデータおよび時間と；

－内部ランダム数と；

－使用者のソフトウェア編集者に属するS_{ε}（『申込データ要項』を意味する$offer_h$、価格）の形態での署名と；

を有することができる。

【００２１】

このメッセージを受領した財布モジュールは、そのような申込内容を承認するかどうかを、使用者（Ｕ）に対して確認する。例えば、申込要項とデータおよび時間と支払金額および通貨とフランスフランに換算した金額とを示すウィンドウが、スクリーン上に表示される。この表示は、図１において矢印（１ａ）によって示されている。

【００２２】

使用者（Ｕ）が申込内容を承認する場合には、使用者は、（例えば）『承認』ボタンをクリックする（この応答は、図１において矢印（１ｂ）によって示されている）。その後、財布モジュールが、サーバ（ＳＰ）に対して、『支払要求』というメッセージ（２）を送信する。このメッセージは、以下のものを有することができる。すなわち、

－申込データ要項$offer_h$、価格、データおよび時間、ランダム数、および、署名S_E（申込データ要項$offer_h$、価格）と；

－使用者（Ｕ）の識別子、および、ソフトウェア編集者（Ｅ）の識別子と；

－申込者が購入を承認した証明書と；

を有することができる。証明書の様式は、発明の実施態様に依存する。すなわち、証明書は、支払サーバ（ＳＰ）に対して送出されるパスワードと、符号化された証明をそれ自体がサーバ（ＳＰ）に対して付与することとなる、ＩＣカード内に含まれた秘密コードと、署名などと、から構成することができる。

【００２３】

申込データ要項（$offer_h$）が、申込完了よりも先に送出されることは、使用者が、サーバ（ＳＰ）によるチェックを妨害することなく、選択したものをサーバ（ＳＰ）に対して明らかにする必要がないことを意味する。

【００２４】

その後、支払要求を受領した（図１において符号（２）によって示されている）支払サーバ（ＳＰ）は、以下の操作を行う。すなわち、

－使用者によって与えられた証明書をチェックし；

－必要であれば、金額をフランスフランへと変換し；

－使用者の消費をチェックし；例えば、サーバ（ＳＰ）が、使用開始からの使用者の合計消費が、使用者に割り当てられた許容上限金額以下であることをチェックしたり（後払い使用者の場合）、あるいは、合計消費が、使用者によって入金された預金残高以下であることをチェックしたり（前払い使用者の場合）し；

－支払要求を記録して、その後の支払操作の実行を可能とする。この場合の記録には、少なくとも以下の情報が、含まれている。すなわち、

－使用者の識別子と；

－ソフトウェア編集者の識別子と；

－価格と；

－データおよび時間、申込データ要項（$offer_h$）、等、

が含まれている。

【００２５】

支払サーバ（ＳＰ）は、支払決定メッセージ（３）を作成する。この支払決定メッセージは、ソフトウェアプログラムおよび『購買』インターフェースに対して、支払が実際に行われたことを証明し、検証可能な証明書を付与する。支払決定メッセージは、以下の情報を有することとなる。すなわち、

－サーバ（ＳＰ）の識別子と；

－支払サーバからの署名S_{SP}（申込データ要項（$offer_h$）、価格、ランダム数、データおよび時間）、

を有することとなる。

【００２６】

財布モジュールは、単に、購買インターフェースへと支払決定メッセージを送信する。

【００２７】

購買インターフェースは、支払決定メッセージの署名S_{SP}（申込データ要項（$offer_h$）、価格、ランダム数、データおよび時間）と、先に送信した申込パラメータと、を照合する。一致した場合には、ソフトウェア（Ｌ）は、継続して使用することができる。

【００２８】

例えば１ヶ月単位といったように定期的に、サーバ（ＳＰ）は、各使用者の合計使用時間を計算する。そして、（後払い使用者に対しては）使用者の取引銀行を介して合計金額の実際の徴収を行う、あるいは、前もってカード番号が知らされているクレジットカードを使用して合計金額の実際の徴収を行う、あるいは、使用者の口座から直接的に合計金額の実際の徴収を行う。

【００２９】

前払い使用者は、媒介手段を介して残高を補給することを選択することによって、支払を行う。

【００３０】

ソフトウェア編集者ごとに計算された合計金額は、各ソフトウェア編集者から借りている金額を同様に計算できることを、意味する。

【００３１】

図１における破線は、サーバ（ＳＰ）からソフトウェア編集者に対しての財務フローに対応している。

【００３２】

上述した様々な署名を設定するために、証明ツリーを有した一般キーを使用したシステムを使用することができる。これは、実際、単純でありかつ安全でありかつ開放的でありかつ国際的に認識されたシステムの形成を可能とする数少ないいくつかの手段のうちの１つである。

【００３３】

この技術の原理は、周知である。この技術の実施態様が、図２に示されている。権威者（Ａ）は、システムの様々な構成要員を有してなる証明ツリーの『根源』を規定する。この場合の構成要員とは、

－この支払手段を使用するソフトウェア編集者と；

－支払サーバと；

－媒介手段と；

である。図２の例においては、媒介手段とは、国のソフトウェア編集者協会（ＳＹＮＤ）と、その国のインターネットサーバを支配している国家的規則権威者（ＳＩＮＴ）と、することができる。

【００３４】

このようにして、あるソフトウェア編集者によって製造されたソフトウェアプログラムが、所定のサーバ（ＳＰ）に対応した使用者によって使用された場合には、メッセージ（１，３）に対して添付される１つまたは複数の証明を使用することにより、署名をチェックすることができる。

【００３５】

申込メッセージ（メッセージ（１））においては、ソフトウェア編集者（Ｅ）は、サーバ（ＳＰ）に対して、申込データ要項$offer_h$、価格、データおよび時間、ランダム数、署名S_E（申込データ要項$offer_h$、価格）、ＳＹＮＤによって送信された、Ｅの証明書、および、Ａによって送信された、ＳＹＮＤの証明書を有したメッセージを、送信することができる。

【００３６】

権威者（Ａ）の一般キーを知っているサーバ（ＳＰ）は、権威者（Ａ）の一般キーを使用することによって、権威者（Ａ）によって送信された、ＳＹＮＤの証明書をチェックする。したがって、サーバ（ＳＰ）は、ＳＹＮＤの一般キーを確実に得ることができ、ＳＹＮＤの一般キーを使用することによって、ＳＹＮＤによって送信された、Ｅの証明書をチェックする。したがって、サーバ（ＳＰ）は、Ｅの一般キーを確実に得ることができ、最終的に、署名S_Eをチェックすることができる。

【００３７】

上記実施形態の変形例は、例えばインターネットを使用することによって使用者が支払要求ごとにサーバ（ＳＰ）に対して接続しなければならないことにより、『オンライン』技術として分類することができる。この変形例は、頻繁ではない支払の場合にのみ可能である（例えば、ＤＶＤ－ＲＯＭ上に２時間映画を受領するような場合）。

【００３８】

本発明は、支払を繰り返す場合により好適な他の形態（第２実施形態）を想定している。この第２実施形態は、図３に図示されている。第２実施形態は、カード読取器（ＬＣ）とカード（Ｃ）との存在を前提としている。カードが安全な媒体であることにより、カードは、メッセージ（２，３）に関して、サーバ（ＳＰ）の役割を代替する。この場合、メッセージ（２，３）は、モジュール（Ｗ）とカード読取器（ＬＣ）との間にわたって送信される。この実施形態は、上記変形例とは異なり、『オフライン』技術として分類することができる。ソフトウェア編集者（Ｅ）は、この場合でも支払サーバ（ＳＰ）から支払を受ける。サーバ（ＳＰ）は、カード内に記録された情報を定期的に受領する（ラインＰＰ）。

【００３９】

カード（Ｃ）は、２つのタイプのものとすることができる。

【００４０】

－１つは、前払いカード（例えば、『電子財布』のタイプ）とすることができる。この場合、残高が、支払メッセージが処理されるごとに減少する。したがって、残高がゼロとなる前にカードが補充されなければならないことにより、未払いとなるリスクがない。しかしながら、ソフトウェアが使用された回数は、記録されなければならない。これにより、使用に応じてソフトウェア編集者に対して支払を行うことができる。これは、例えば、カードが再挿入される際に、行われる。

【００４１】

－他は、後払いカードとすることができる。この場合、カード内に記録されたソフトウェアの使用が、媒介手段に到達することがなく、そのため使用者が支払を行わず、その結果、使用されたソフトウェアの編集者が決して保証されていないというリスクがある。この問題点を解決するために、支払をある上限に制限し、また、その上限よりも大きくなった場合に使用者に支払を求め、使用者にカードを『紛失』させないようにする。

【００４２】

使用されている厳密な機構という観点において、第２実施形態は、第１実施形態と非常に類似している。相違しているのは、サーバ（ＳＰ）の機能が、カード（Ｃ）によって代替されている点である。したがって、このカードは、すべての使用を記録したファイルを備えなければならず、サーバ（ＳＰ）の場合と同様に、実行記録を備えている。この実行記録には、少なくとも、

－使用者の識別子と、

－ソフトウェア編集者の識別子と、

－価格と、

が、含まれている。

【００４３】

カード読取器にかかる付加的なコストを避けるために、わずかの安全性の低減

が許容される場合には、カードは、ＰＣ内の記憶手段によって代替することができる。

【００４４】

支払要求ファイルが容易に変更されたり容易に消去されたりしないように、ディスク全体にわたって情報の分散化を行うという技術が使用されなければならない。ディスクの完全性が、障壁をもたらす。実際には、ＩＣカードによってもたらされる物理的安全性よりは弱いものの、多くの場合には、十分である。

【図面の簡単な説明】

【図１】　本発明の第１実施形態によるシステムを示す図である。

【図２】　証明チェインを有してなる証明ツリーを示す図である。

【図３】　本発明の第２実施形態によるシステムを示す図である。

【符号の説明】

１　申込メッセージ（第１メッセージ）

２　第２メッセージ

３　支払決定メッセージ

Ａ　権威者

Ｃ　カード（ＩＣカード、（静止手段）

Ｅ　ソフトウェア編集者

ＩＬ　ソフトウェアインターフェース

Ｌ　ソフトウェアプログラム

ＬＣ　カード読取器（ＩＣカード読取器、静止手段）

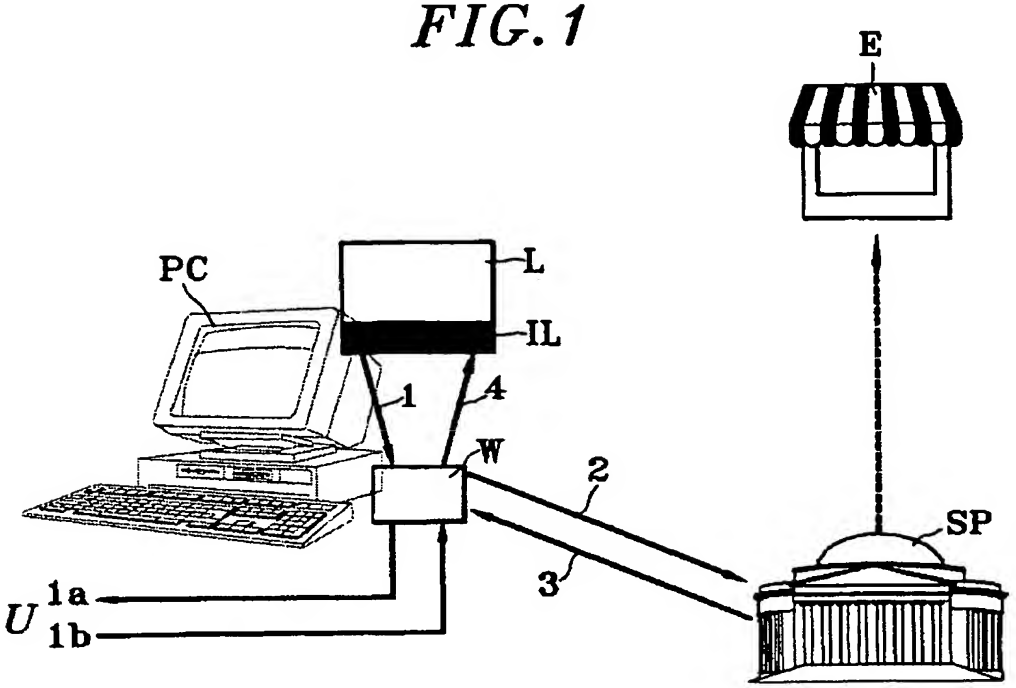
ＳＰ　支払サーバ（遠隔支払サーバ、メッセージ送受信可能な支払手段）

Ｕ　使用者

Ｗ　支払モジュール

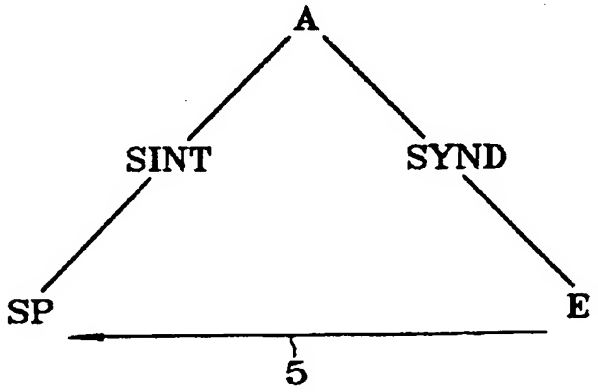
【図１】

FIG. 1



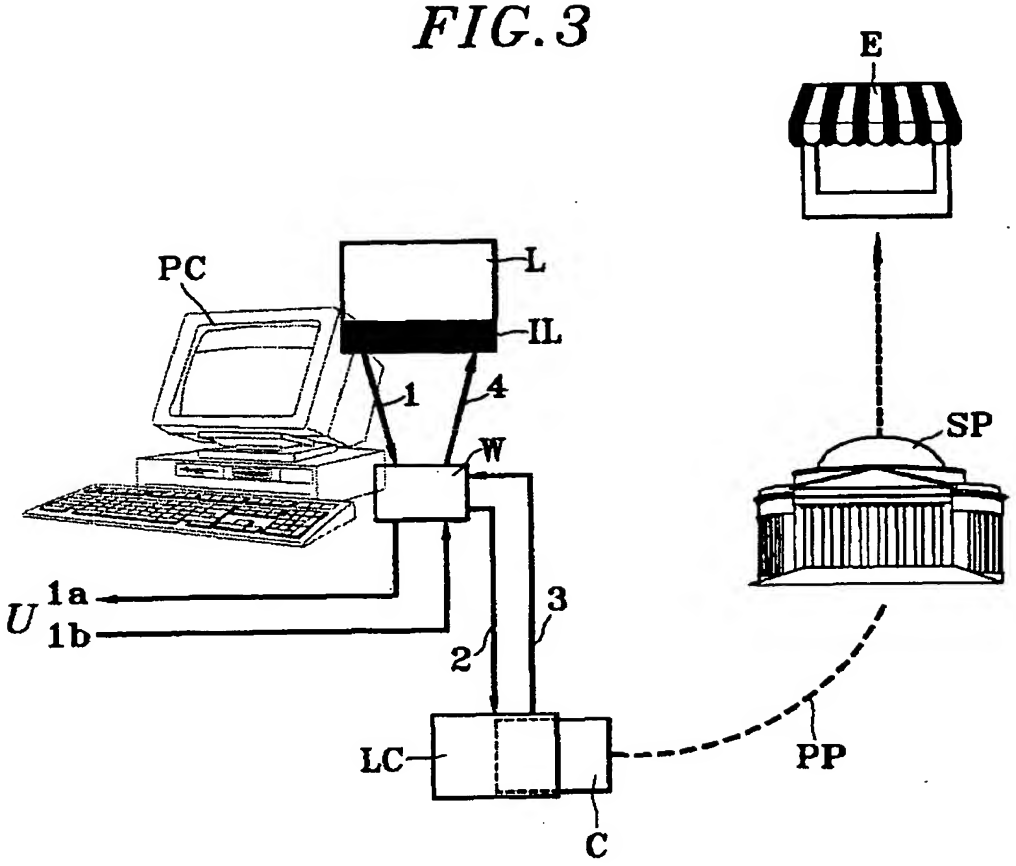
【図２】

FIG. 2



【図３】

FIG.3



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/FR 00/01023

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G07F17/16 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04N G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 95 34857 A (SMITH JAMES P ;SMITH EDWARD A (US)) 21 December 1995 (1995-12-21) page 6, line 1 - line 5 page 6, line 26 -page 7, line 18 page 8, line 6 - line 18 page 8, line 26 -page 9, line 5 page 9, line 29 -page 10, line 5 page 10, line 34 -page 11, line 12 page 11, line 32 -page 12, line 25; claim 1; figures 2,6,7 abstract --- -/--	1,3-5, 14-16 2,6-13, 17-22

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2000	25/07/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Wauters, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. Local Application No
PCT/FR 00/01023

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 809 221 A (SUN MICROSYSTEMS INC) 26 November 1997 (1997-11-26) column 1, line 3 - line 7 column 1, line 18 - line 27 column 2, line 49 -column 3, line 6 column 4, line 9 - line 11 column 4, line 39 - line 49 column 5, line 1 - line 49 column 6, line 2 -column 7, line 39 column 8, line 10 - line 18 column 9, line 56 -column 10, line 37; claim 1; figures 1,2,4-6,8 abstract	1,3,4, 14,15 2,5-13, 16-22
Y A	US 5 769 269 A (PETERS STEVEN A) 23 June 1998 (1998-06-23) column 1, line 18 - line 21 column 2, line 49 - line 56 column 8, line 13 - line 24; claim 1; figure 1A abstract	6-13, 17-22 1-5, 14-16
Y	US 4 881 264 A (MERKLE RALPH C) 14 November 1989 (1989-11-14) column 2, line 59 - line 68 column 3, line 19 - line 38; figures 1-3 abstract	2
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 312277 A (NAKAMICHI CORP), 24 November 1998 (1998-11-24) abstract	1-22

Form PCT/ISA/210 (continuation of second sheet)(July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/01023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9534857 A	21-12-1995	AU 2774495 A	05-01-1996
EP 0809221 A	26-11-1997	JP 10222579 A	21-08-1998
US 5769269 A	23-06-1998	AU 2466095 A	29-11-1995
		BR 9507545 A	05-08-1997
		GB 2303238 A,B	12-02-1997
		WO 9530212 A	09-11-1995
US 4881264 A	14-11-1989	NONE	
JP 10312277 A	24-11-1998	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(72)発明者 ステファン・ベティ
フランス・Ｆ－14470・クールスール／メル・リュ・ドゥ・ヴェル・32・レジダンス・デュ・ヌーヴォー・バサン・バティン・レ・ジリ・アバルトマン・146

Ｆターム(参考) 5B058 CA27 KA02 KA04 KA31 KA02
YA20
5B076 FB01 FB10 FC